

CLAIMS

1. A system for authentication of a party comprising:

an authentication server associating a unique set of information with said party, said unique set including at least a unique ordered set of information randomly generated; responsive to receipt of identifying information of said party to determine by random generation values of one or more prescribed parameters to define an ordered subset of said ordered set, to transmit said values, to generate a first token from said ordered subset, to compare said first token to a second token received in response to said transmission, and upon a match, to authenticate said party; and

a separate processor operated by said party adapted to read locally a storage medium containing a copy of said unique set of information associated by said server with said party, to transmit to said server said identifying information, to receive said values from said server, to apply said values to define an ordered subset of said copy, and to transmit said second token generated from said ordered subset of said copy.

2. The system of claim 1 wherein said first token includes personal code known to said party and stored and associated with said party at said server and said second token identically includes said personal code entered by said party at said separate processor.

3. The system of claim 1 wherein said server further comprises means for, upon said match, generating and storing a transaction token and transmitting to said processor said transaction

1 token; said system further comprising an authentication-seeking entity adapted to receive
2 from said processor said transaction token, to transmit said transaction token to said server,
3 and to receive from said server authentication upon match by said server of said stored
4 transaction token with said transmitted transaction token.

5
6 4. The system of claim 1 further comprising an authentication-seeking entity adapted to
7 receive from said processor said second token, to transmit said second token to said server,
8 and to receive from said server authentication upon match by said server of said first token.

9
10 5. An authentication server associating a unique set of information with a party to be
11 authenticated, said unique set including at least a unique ordered set of information randomly
12 generated; said server responsive to receipt of identifying information of said party to
13 determine by random generation values of one or more prescribed parameters to define an
14 ordered subset of said ordered set, to transmit said values, to generate a first token from said
15 ordered subset, to compare said first token to a second token received in response to said
16 transmission, and upon a match, to authenticate said party.

17
18 6. The authentication server of claim 5 wherein said first token includes personal code
19 known to said party and stored and associated at said server with said party.

1 7. A processor operated by a party to be authenticated, said processor adapted to read
2 locally a storage medium containing a copy of a unique set of information associated by a
3 separate authentication server with said party, to transmit to said server information
4 identifying said party, to receive from said server values of one or more prescribed
5 parameters to define an ordered subset of said copy, and to transmit to said server a token
6 generated from said ordered subset of said copy.

7

8 8. The processor of claim 7 wherein said token includes personal code known to said party
9 and stored and associated with said party at said server, said processor further comprising
10 means for receiving entry by said party of said personal code.

11

12 9. A computer program product for server-side authentication of a party, said computer
13 program product residing on a computer-readable medium comprising instructions for causing
14 a computer: to associate a unique set of information with a party to be authenticated, said
15 unique set including at least a unique ordered set of information randomly generated; to
16 receive identifying information of said party; to determine in response to such receipt by
17 random generation values of one or more prescribed parameters to define an ordered subset of
18 said ordered set; to transmit said values; to generate a first token from said ordered subset; to
19 receive a second token; to compare said first token to a second token received in response to
20 said transmission; and, upon a match, to authenticate said party.

21

1 10. The computer program product of claim 9 wherein said unique set of information
2 associated with said party further comprises personal code known to said party and said
3 instructions further comprise instructions to generate said first token from both said ordered
4 subset and said personal code.

5
6 11. A computer program product for client-side authentication of a party, said computer
7 program product residing on a computer-readable medium comprising instructions for causing
8 a computer: to read locally a storage medium containing a copy of a unique set of information
9 associated by a separate authentication server with said party; to transmit to said server
10 information identifying said party; to receive from said server values of one or more
11 prescribed parameters to define an ordered subset of said copy; to generate a token from said
12 ordered subset of said copy; and to transmit to said server said token.

13
14 12. The computer program product of claim 11 further comprising instructions: to receive
15 entry by said party of personal code stored and associated with said party at said server; and
16 to generate said token from both said ordered subset and said entered personal information.

17
18 13. A process for authenticating a party comprising selection at a central location of a
19 randomly selected portion of random information uniquely associated with said party,
20 parallel selection at a party location separate from said central location an identical portion of
21 a putatively identical copy of said information issued to and possessed by said party, and

1 comparison at said central location of a first token uniquely generated from said randomly
2 selected portion with a second token uniquely generated from said identically selected
3 portion.

4
5 14. The process of claim 13 wherein said first token includes personal code known to said
6 party and stored and associated with said party at said central location and said second token
7 identically includes said personal code entered by said party at said separate location.

8
9 15. A process for authenticating a party comprising the steps of:

10 (a) accessing by said party through a client computer of an authentication
11 server that has stored random information uniquely associated with said party, a copy
12 of which was previously provided to said party and accessible at the client side;

13 (b) generating by said server or said client at least one random value for an
14 authentication session of a parameter for selecting an ordered subset of said stored
15 random information;

16 (c) transmitting by said server or client respectively to said client or server
17 said generated value;

18 (d) applying by said client said generated value or values to select an ordered
19 subset of said copy information;

20 (e) generating by said client from said ordered subset of copy information a
21 client-side party-authenticating token;

1 (f) applying by said server of said generated value or values to select an
2 ordered subset of said stored information;

3 (g) generating by said server from said ordered subset of stored information a
4 server-side party-authenticating token;

5 (h) transmitting by said client to said server said client-side token or by said
6 server to said client said server-side token; and

7 (i) comparing by said server said client-side token with said server-side token
8 or by said client said server-side token with said client-side token.

9 16. The process of claim 15 wherein step (b) comprises the steps of generating random
10 values for an offset, a length and a shift; and steps (e) and (g) each comprise the step of
11 applying a specified one-way hashing algorithm to generate respectively said client-side and
12 server-side party-authenticating tokens.

13
14 17. The process of claim 15 wherein a copy of personal code known to said party is stored
15 and associated with said party at said server and wherein

16 step (e) further comprises the steps of (I) concatenating said ordered subset of
17 copy information and said personal code entered by said party and (II) applying a
18 specified one-way hashing algorithm to generate said client-side party-authenticating
19 token; and

20 step (g) further comprises the steps of (I) concatenating said ordered subset of
21 stored random information and said personal code copy and (II) applying said

1 specified one-way hashing algorithm to generate said server-side party-authenticating
2 token.

3
4 18. The process of claim 17 wherein step (b) comprises the steps of generating random
5 values for an offset, a length and a shift.

6
7 19. The process of claim 18 wherein step (b) further comprises selection of a one-way hash
8 algorithm.

9
10 20. The process of claim 15 wherein a copy of personal code known to said party is stored
11 and associated with said party at said server and wherein
12 step (e) further comprises the steps of (I) dividing said ordered subset of copy
13 information into first and second portions; (II) concatenating each of said first and
14 second portions with said personal code entered by said party; (III) applying a
15 specified one-way hashing algorithm to said concatenation of said first portion to
16 generate said client-side party-authenticating token; and (IV) applying said specified
17 one-way hashing algorithm to said concatenation of said second portion to generate a
18 second client-side party-authenticating token;

19 step (g) further comprises the steps of (I) dividing said ordered subset of
20 stored random information into first and second portions corresponding to said first
21 and second portions of step (b); (II) concatenating each of said first and second

1 portions of this step with said personal code copy; (III) applying said specified one-
2 way hashing algorithm to said concatenation of said first portion to generate said
3 server-side party-authenticating token; and (IV) applying said specified one-way
4 hashing algorithm to said concatenation of said second portion to generate a second
5 server-side party-authenticating token;

6 step (h) is performed by said client;

7 step (i) is performed by said server; and,

8 wherein, if step (i) results in a match, said process further comprises the steps of

9 (j) transmitting by said server to said client said second server-side token; and

10 (k) comparing by said client of said server-side token with said client-side

11 token.

12
13 21. The process of claim 20 wherein step (b) comprises the steps of generating random
14 values for an offset, a length and a shift.

15
16 22. The process of claim 21 wherein step (b) further comprises selection of a one-way hash
17 algorithm.

18
19 23. The process of claim 15 applied to authenticating said party to an authentication-seeking
20 entity in a transaction wherein, if step (i) results in a match, said process further comprises

21 the steps of

1 (j) generating by said server a transaction token;
2 (k) storing at said server a copy of said transaction token associated with said
3 party;
4 (l) transmitting by said server to said client said transaction token;
5 (m) transmitting by said client to said authentication-seeking entity said
6 transaction token received from said server;
7 (n) transmitting by said authentication-seeking entity to said server said
8 transaction token received from said client;
9 (o) comparing by said server of said transaction token received from said
10 authentication-seeking entity with said copy of said transaction token associated with
11 said party.

12
13 24. The process of claim 15 applied to authenticating said party to an authentication-seeking
14 entity in a transaction wherein, if step (i) results in a match, said process further comprises
15 the steps of

16 (j) generating by said server a server-side transaction authentication token from
17 information associated with said party and stored at said server;
18 (k) transmitting by said server to said client information to specify parallel
19 generation by said client of a client-side transaction authentication token from
20 corresponding information made available at said client ;

1 (l) generating by said client said client-side transaction token from said
2 corresponding information;

3 (m) transmitting by said client to said authentication-seeking entity said
4 client-side transaction token;

5 (n) transmitting by said authentication-seeking entity to said server said
6 client-side transaction token received from said client;

7 (o) comparing by said server of said client-side transaction token received from
8 said authentication-seeking entity with said server-side transaction token associated
9 with said party.
10

11 25. The process of claim 15 applied to authenticating work product that said party creates
12 or modifies using said client computer wherein, if step (i) results in a match, said process
13 further comprises the steps of

14 (j) generating by said server a work-product-authentication token;

15 (k) storing at said server a copy of said work-product-authentication token
16 associated with said party;

17 (l) attaching to said work product said work-product-authentication token to
18 create a data object stored and movable as authenticated work product;

19 (m) storing said authenticated work product;

20 (n) extracting from said authenticated work product a putative work-product
21 authentication token; and

1 (o) comparing at said server said stored work-product-authentication token
2 with said putative work-product-authentication token.
3

4 26. The process of claim 15 applied to authenticating work product that said party creates
5 or modifies using said client computer wherein, if step (i) results in a match, said process
6 further comprises the steps of

7 (j) generating by said server a server-side work-product-authentication token
8 from information associated with said party and stored at said server;

9 (k) transmitting by said server to said client information to specify parallel
10 generation by said client of a client-side work-product-authentication token from
11 corresponding information made available at said client;

12 (l) generating by said client said client-side work-product-authentication token
13 from said corresponding information;

14 (m) attaching to said work product said client-side work-product-
15 authentication token to create a data object stored and movable as authenticated work
16 product;

17 (n) storing said authenticated work product;

18 (o) extracting from said authenticated work product said client-side work-
19 product authentication token; and

20 (p) comparing at said server said serve-side work-product-authentication
21 token with said client-side work-product-authentication token.

1

2 27. The process of claim 15 applied to authenticating said party for access to a restricted
3 resource wherein, if step (i) results in a match, said process further comprises the step of
4 (j) transmitting by said server authorization to permit said access.

5

6 28. The process of claim 15 applied to authenticating said party for access at said client to a
7 restricted resource wherein

8 step (h) is performed by said server;

9 step (i) is performed by said client; and

10 if step (i) results in a match, said process further comprises the step of

11 (j) permitting by said client of access to said resource.

12

13 29. The process of claim 15 applied to authenticating said party for continuing access to a
14 restricted resource wherein said copy is normally separate from and inaccessible by said
15 client except when connected through action of said party and steps (b) through (i) are
16 repeated periodically until step (i) fails to result in a match a predetermined number of times.

17